A New Paradigm for Automated Development of Highly Reliable Control Architectures for Nuclear Power Plants

R. T. Wood, J. March-Leuba; Oak Ridge National Laboratory
B. R. Upadhyaya; University of Tennessee, Knoxville
J. M. Doster, C. W. Mayo; North Carolina State University

Nuclear reactors of the 21st century will employ increasing levels of automation and fault tolerance to increase availability, reduce accident risk, and lower operating costs. Key developments in control algorithms, fault diagnostics, fault tolerance, and distributed communications are needed to implement the fully automated plant. Equally challenging will be integrating developments in separate information and control fields into a cohesive system, which collectively achieves the overall goals of improved safety, reliability, maintainability, and cost-effectiveness. Under the Nuclear Energy Research Initiative (NERI), the U. S. Department of Energy is sponsoring a project to address some of the technical issues involved in meeting the long-range goal of 21st century nuclear plant control system. This project involves researchers from Oak Ridge National Laboratory, University of Tennessee, and North Carolina State University. The research tasks under this project focus on some of the first level breakthroughs in control design, diagnostic techniques, and information system design that will provide a path to enable the design process to be automated in the future.

The primary goal of this research is to develop methods for automated design of highly reliable control systems. To this end, we endeavor to develop an automated control "engine," which is capable of drawing upon a library of control algorithms to generate a control design that meets all design requirements. This is accomplished by minimizing a user-defined cost function subject to the constraints imposed by the requirements. The user also defines in advance a set of stress factors, such as single-failure criteria, or a list of plant transients that the control system must be able to accommodate.

Automating the control system design is a significant accomplishment, especially when satisfaction of the design requirements can be confirmed as part of the process. However, the control engine methodology can also be used in a supervisory mode during operation. As the plant conditions change (e.g., component failures or changes in operating mode) the control engine automatically tests all original requirements and either adapts the control system design or employs new control algorithms, as necessary, to meet the control objectives.

To accomplish this goal, we are conducting research in four major areas: (1) Accurate plant models are required to implement the methodology. (2) A means for continuously verifying the accuracy of these plant models and adapting to changing conditions is needed; this can only be accomplished through on-line diagnostics. (3) The control engine methodology itself must be developed and tested. (4) Finally, the complete system must use flexible, reliable control architectures to accommodate on-line optimization while preventing implementation errors. Progress has been achieved in each of these areas during the first year of this research project.